Patent Application

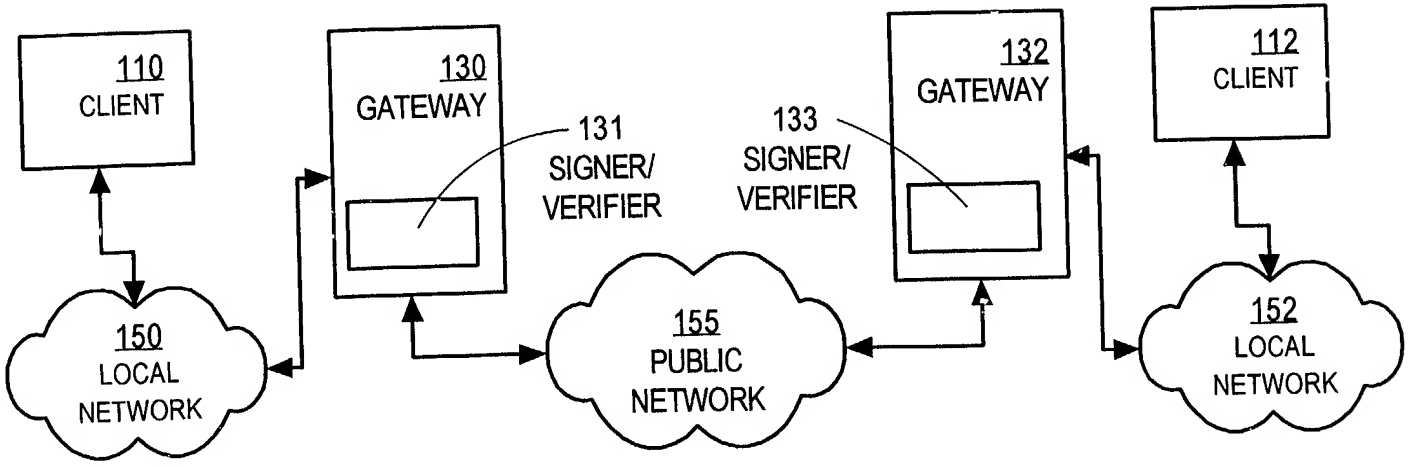


FIG. 1A

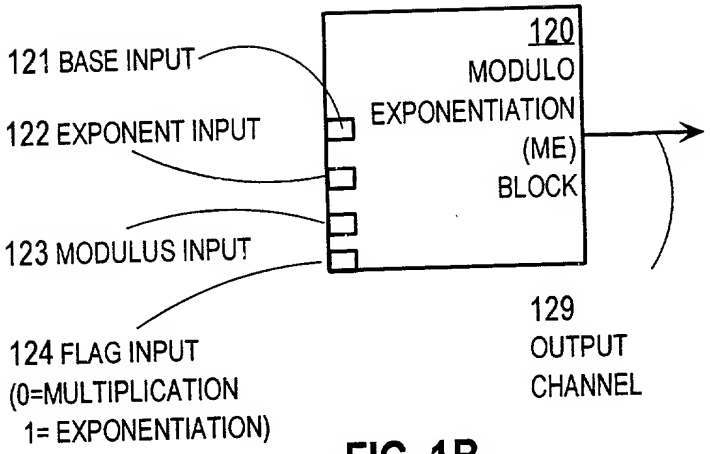

120
MODULO
EXPONENTIATION
(ME)
BLOCK
121 BASE INPUT
122 EXPONENT INPUT
123 MODULUS INPUT
124 FLAG INPUT
(0=MULTIPLICATION
1= EXPONENTIATION)
129
OUTPUT
CHANNEL

FIG. 1B

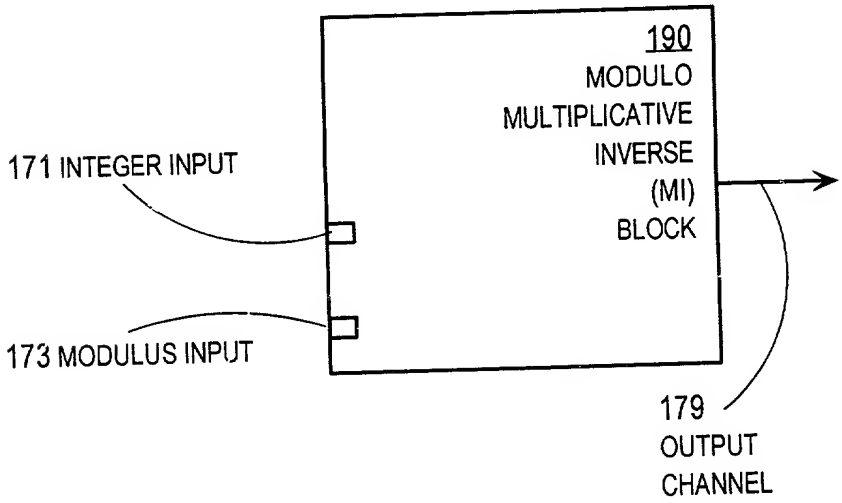

190
MODULO
MULTIPLICATIVE
INVERSE
(MI)
BLOCK
171 INTEGER INPUT
173 MODULUS INPUT
179
OUTPUT
CHANNEL

FIG. 1C

Patent Application

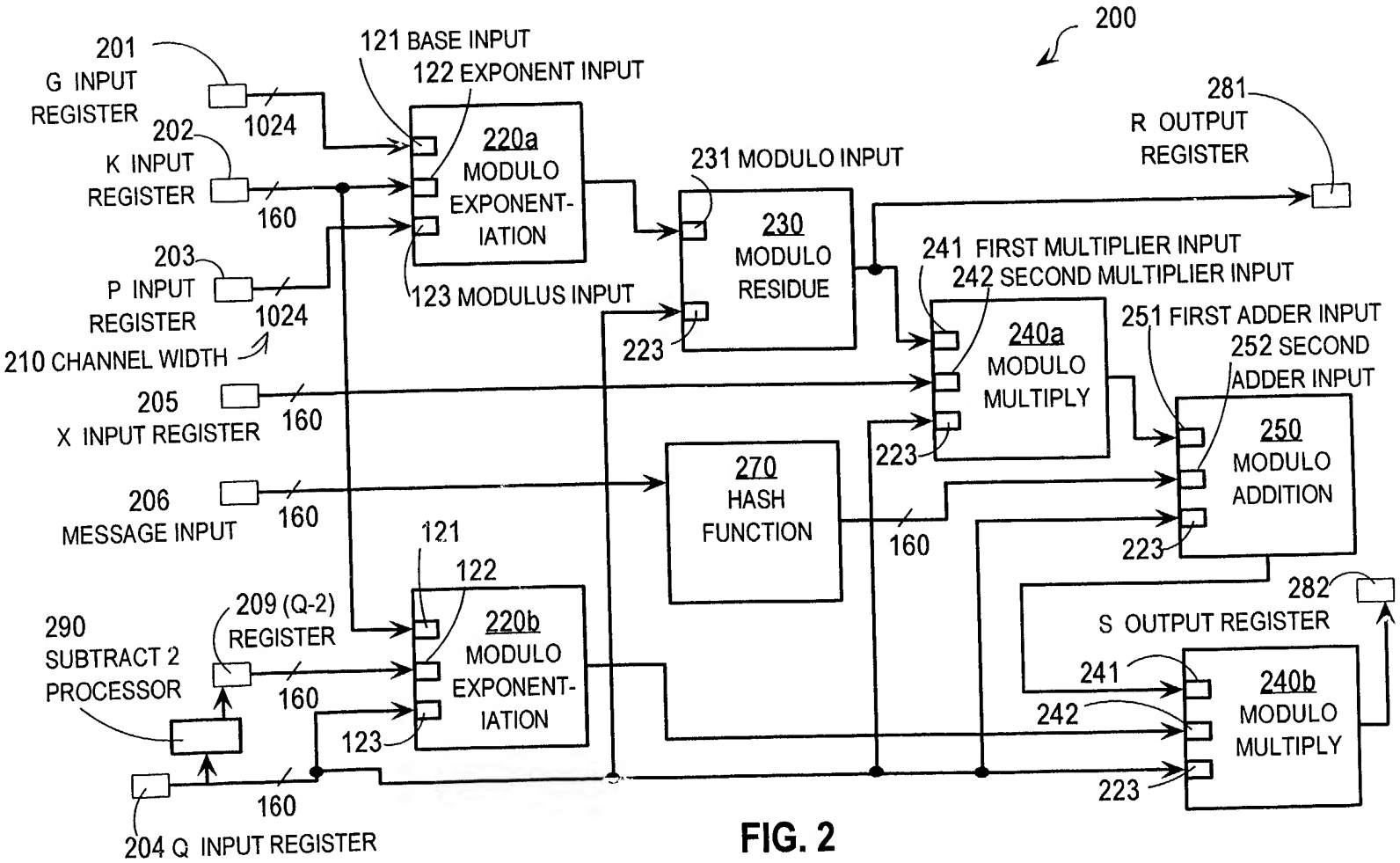


FIG. 2

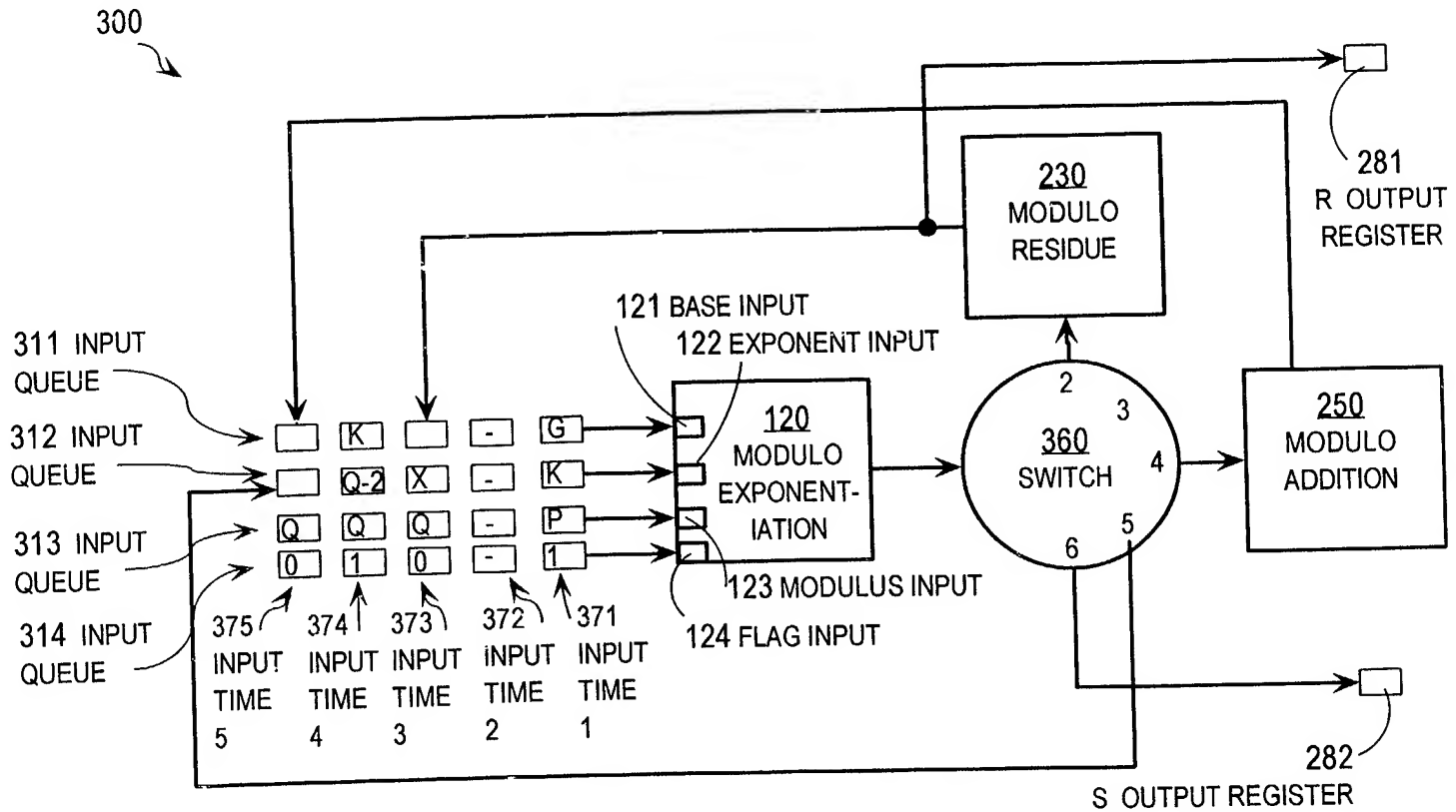

300
230
MODULO
RESIDUE
281
R OUTPUT
REGISTER
121 BASE INPUT
122 EXPONENT INPUT
311 INPUT
QUEUE
312 INPUT
QUEUE
313 INPUT
QUEUE
314 INPUT
QUEUE
K
Q-2
Q
0
X
1
-
G
K
P
1
120
MODULO
EXPONENT-
IATION
123 MODULUS INPUT
124 FLAG INPUT
2
3
360
SWITCH
4
5
6
250
MODULO
ADDITION
375
INPUT
TIME
5
374
INPUT
TIME
4
373
INPUT
TIME
3
372
INPUT
TIME
2
371
INPUT
TIME
1
282
S OUTPUT REGISTER

FIG. 3

FIG. 4

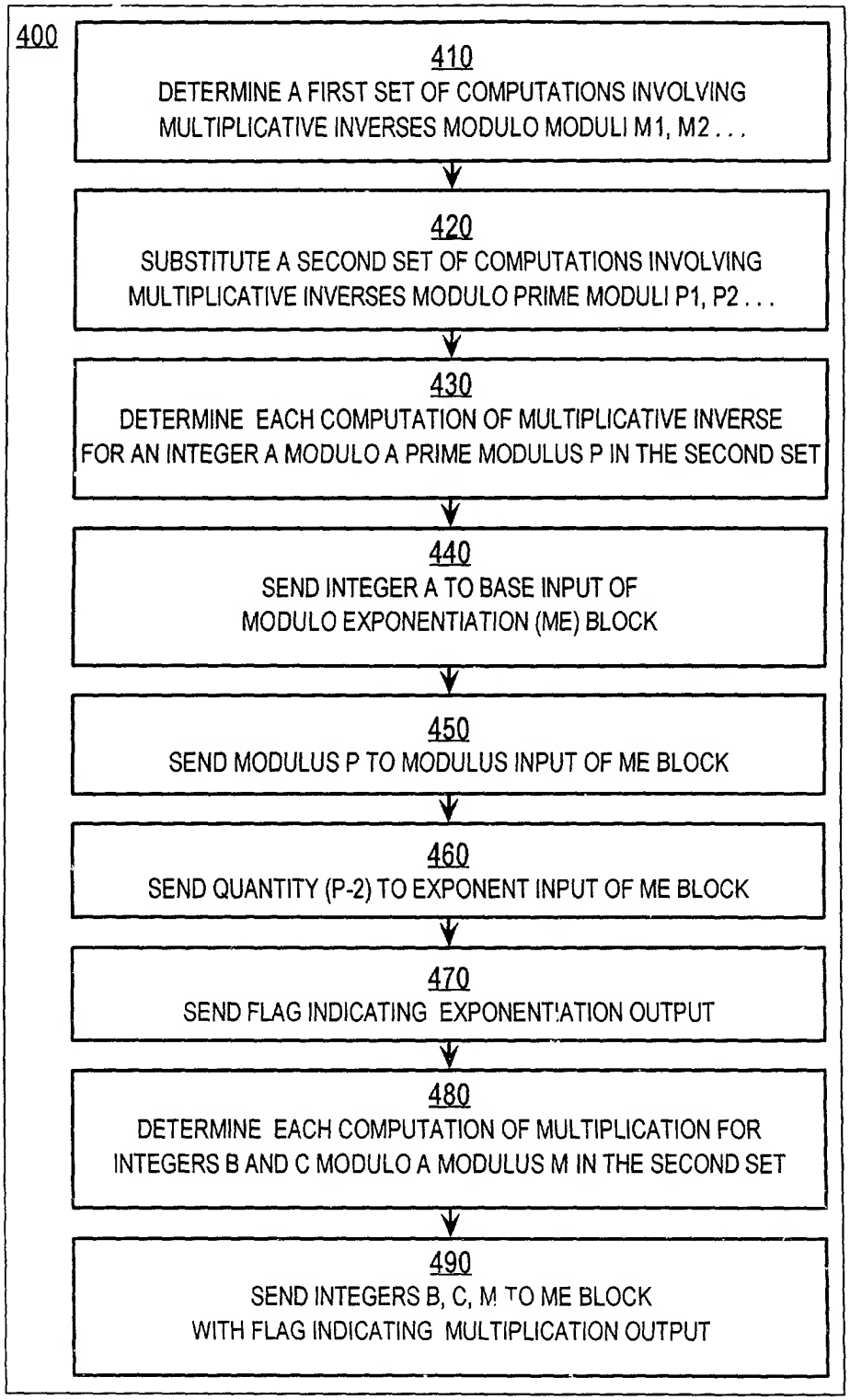
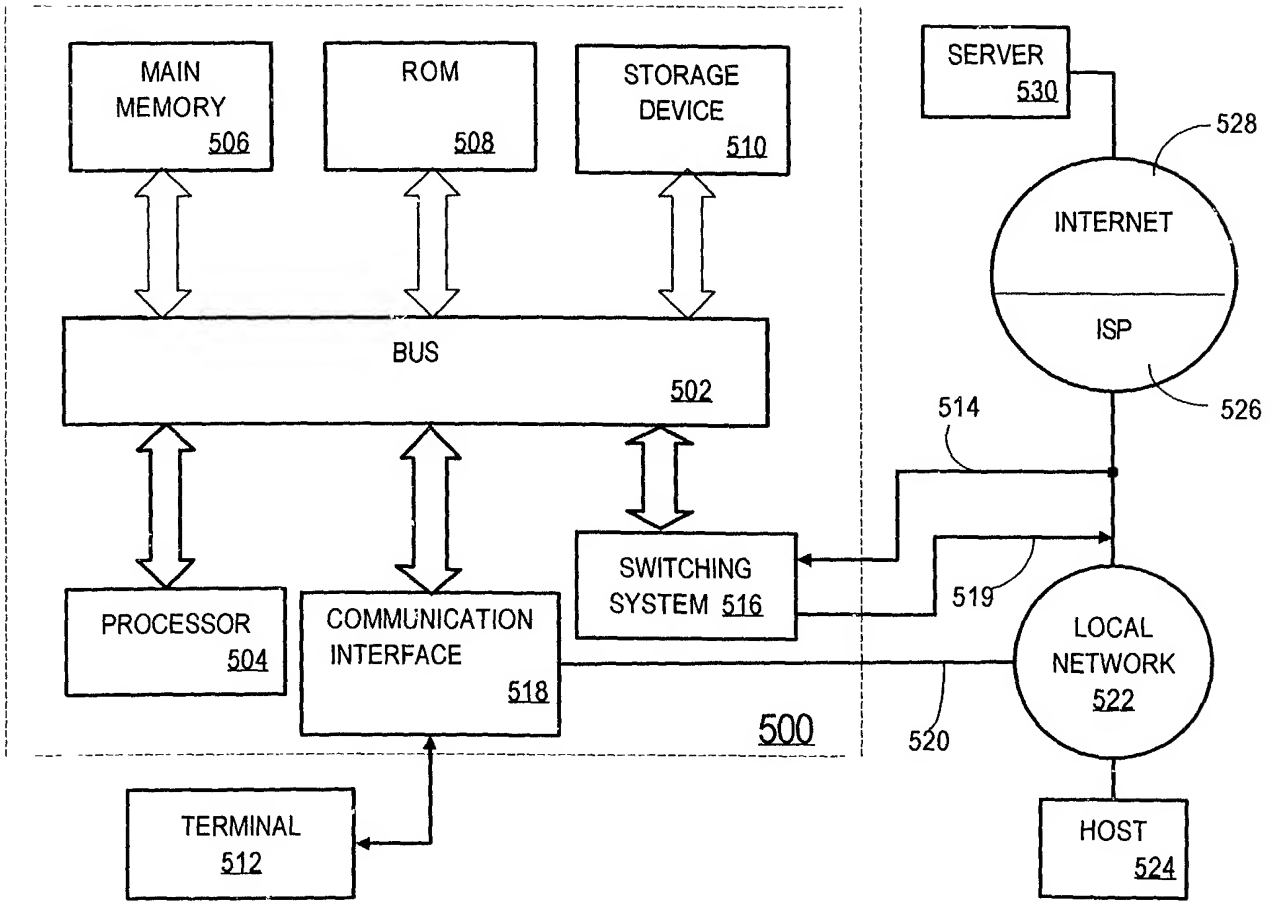

400
410
DETERMINE A FIRST SET OF COMPUTATIONS INVOLVING MULTIPLICATIVE INVERSES MODULO MODULI M1, M2 . . .
420
SUBSTITUTE A SECOND SET OF COMPUTATIONS INVOLVING MULTIPLICATIVE INVERSES MODULO PRIME MODULI P1, P2 . . .
430
DETERMINE EACH COMPUTATION OF MULTIPLICATIVE INVERSE FOR AN INTEGER A MODULO A PRIME MODULUS P IN THE SECOND SET
440
SEND INTEGER A TO BASE INPUT OF MODULO EXPONENTIATION (ME) BLOCK
450
SEND MODULUS P TO MODULUS INPUT OF ME BLOCK
460
SEND QUANTITY (P-2) TO EXPONENT INPUT OF ME BLOCK
470
SEND FLAG INDICATING EXPONENTIATION OUTPUT
480
DETERMINE EACH COMPUTATION OF MULTIPLICATION FOR INTEGERS B AND C MODULO A MODULUS M IN THE SECOND SET
490
SEND INTEGERS B, C, M TO ME BLOCK WITH FLAG INDICATING MULTIPLICATION OUTPUT

FIG. 5


MAIN MEMORY 506
ROM 508
STORAGE DEVICE 510
BUS 502
PROCESSOR 504
COMMUNICATION INTERFACE 518
SWITCHING SYSTEM 516
TERMINAL 512
500
SERVER 530
528
INTERNET
ISP
526
514
519
LOCAL NETWORK 522
520
HOST 524